A Generalized Criterion for Signature-based Algorithms to Compute Gröbner Bases ☆

Yao Sun, Dingkang Wang

Key Laboratory of Mathematics Mechanization
Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China

Abstract

A generalized criterion for signature-based algorithms to compute Gröbner bases is proposed in this paper. This criterion is named by "generalized criterion", because it can be specialized to almost all existing criteria for signature-based algorithms which include the famous F5 algorithm, F5C, extended F5, G^2V and the GVW algorithm. The main purpose of current paper is to study in theory which kind of criteria is correct in signature-based algorithms and provide a generalized method to develop new criteria. For this purpose, by studying some key facts and observations of signature-based algorithms, a generalized criterion is proposed. The generalized criterion only relies on a partial order defined on a set of polynomials. When specializing the partial order to appropriate specific orders, the generalized criterion can specialize to almost all existing criteria of signature-based algorithms. For *admissible* partial orders, a proof is presented for the correctness of the algorithm that is based on this generalized criterion. And the partial orders implied by the criteria of F5 and GVW are also shown to be admissible. More importantly, the generalized criterion provides an effective method to check whether a new criterion is correct as well as to develop new criteria for signature-based algorithms.

Keywords: Gröbner basis, F5, signature-based algorithm, criterion.

1. Introduction

Gröbner basis was first proposed by Buchberger in 1965. Since then, many important improvements have been made to speed up the algorithms for computing Gröbner basis (Buchberger, 1979, 1985; Gebauer and Moller, 1986; Giovini et al., 1991; Möller et al., 1992; Faugère, 1999, 2002). One important improvement is that Lazard pointed out the connection between a Gröbner basis and linear algebra (Lazard, 1983). This idea is also implemented as

☆This paper is a substantially expanded version of the paper entitled "A Generalized Criterion for Signature Related Gröbner Basis Algorithms", which was presented at ISSAC 2011 (Sun and Wang, 2011).

Email address: sunyao@amss.ac.cn, dwang@mmrc.iss.ac.cn (Yao Sun, Dingkang Wang)

[1]The authors are supported by NKBRPC 2011CB302400, NSFC 10971217 and 60821002/F02.

XL type algorithms by Courtois et al. (Courtois et al., 2000) and Ding et al. (Ding et al., 2008). Up to now, F5 is one of the most efficient algorithms for computing Gröbner basis. The notion of "signatures" for polynomials was also introduced by Faugère in (Faugère, 2002). Since F5 was proposed in 2002, it has been widely investigated and several variants of F5 have been presented, including the F5C algorithm (Eder and Perry, 2010) and F5 with extended criteria (Hashemi and Ars, 2010). Proofs and other extensions of F5 are also investigated in (Stegers, 2006; Eder, 2008; Albrecht and Perry, 2010; Arri and Perry, 2010; Sun and Wang, 2010a,b; Zobnin, 2010). Recently, Gao et al. proposed an incremental signature-based algorithm G^2V to compute Gröbner basis in (Gao et al., 2010a), and presented an extended version GVW in (Gao et al., 2010b). The framework of signature-based algorithms was studied in (Eder and Perry, 2011).

The common characteristics of F5, F5C, extended F5, G^2V and GVW are (1) each polynomial has been assigned a *signature*, and (2) both the criteria and the reduction process depend on the signatures of polynomials. So all these algorithms are signature-based algorithms. The only difference among the algorithms is that their criteria are different.

By studying these criteria carefully, we find a key fact in signature-based algorithms, and then some observations are motivated. One key observation is that if two polynomials have the same signature, then at most one of them is necessary to be reduced. The reason is that reducing two polynomials that have the same signature, could create the same leading power product if some extra conditions hold. With this insight, we use a partial order to help choose one polynomial that is not to be reduced. Then a generalized criterion for signature-based algorithms is proposed based on this partial order. By using appropriate partial orders, the generalized criterion can be specialized to almost all existing criteria of signature-based algorithms.

Unfortunately, not all partial orders can make the generalized criterion correct. We proved that the generalized criterion is correct if the partial order is *admissible*. Moveover, we show that the partial orders implied by F5 and GVW's criteria are both admissible, so the proof in this paper is also valid for the correctness of F5 and GVW.

The significance of the generalized criterion is to show which kind of criteria is correct for signature-based algorithms and provide a generalized method to check or even develop new criteria. Specifically, when a new criterion is presented, if it can be specified from the generalized criterion by using an admissible partial order, then this new criterion is definitely correct. It is also possible for us to develop some new criteria by using new admissible partial orders in the generalized criterion. From the proof in this paper, we know that any admissible partial order can develop a new criterion for signature-based algorithms in theory, but not all of these criteria can reject as many critical pairs as possible. Therefore, we believe that if the admissible partial order is in fact a total order, then almost all useless computations can be avoided. The proof for the claim will be included in our future works.

The paper is organized as follows. We present our main ideas of the generalized criterion in Section 2. Section 3 gives the generalized criterion and shows how this generalized criterion is used. Section 4 details how the generalized criterion specializes to F5 and GVW's criteria. We prove the correctness of the generalized criterion in Section 5. A new criterion is developed in Section 6. Concluding remarks follow in Section 7.

2. Main ideas

2.1. Problem

Let $R := \mathrm{K}[x_1, \cdots, x_n]$ be a polynomial ring over a field K with n variables. Suppose $\{f_1, \cdots, f_m\}$ is a finite subset of R. We want to compute a Gröbner basis for the ideal

$$I := \langle f_1, \cdots, f_m \rangle = \{p_1 f_1 + \cdots + p_m f_m \mid p_1, \cdots, p_m \in R\}$$

with respect to some term order on R.

Fix a term order $\prec_1$ on R. We define the *leading power product* and *leading coefficient* of a polynomial $f \in R$ to be $\mathrm{lpp}(f)$ and $\mathrm{lc}(f)$ in general way. For example, let $f := 2x^2y + 3z \in \mathbb{Q}[x, y, z]$ where $\mathbb{Q}$ is the rational field. Then $\mathrm{lpp}(f) = x^2y$ and $\mathrm{lc}(f) = 2$.

As we know, a set $G \subset I$ is a Gröbner basis for I, if and only if

$$\langle \mathrm{lpp}(G) \rangle = \langle \mathrm{lpp}(I) \rangle.$$

That is, a Gröbner basis should contain all the leading power product information of I. So in order to compute a Gröbner basis for I, all existing algorithms start with a set of known generators, and then a Gröbner basis can be obtained by expanding these known generators constantly with polynomials having new leading power products. To get the polynomials that have new leading power products, the only way is to *reduce* polynomials in I. However, if a polynomial is reduced to 0, then this reduction is redundant, since no new leading power product appears. In this case, criteria for Gröbner basis algorithms are created, and *all criteria aim to avoid computations that reduce polynomials to* 0.

Now we should answer an important question: given $f \in I$ and $G \subset I$, **how can we *predict* the reducing result of f by G without really reducing it?**

Signature-based algorithms give a good solution to this question, and we notice that their common methods are based on **ordering the polynomials in I according their signatures in order to get a beautiful property**. This beautiful property is a key fact in signature-based algorithms, and it will be presented in Subsection 2.3. First, let us see what is the signature of a polynomial in I.

2.2. Signature

We will use the following simple example to help illustrate some notions in this subsection, and these notions can be extended to general case easily.

Example 2.1. *Let $I := \langle f_1, f_2, f_3 \rangle$ be an ideal in the polynomial ring $R = \mathbb{Q}[x, y, z]$, where $f_1 = yz - x$, $f_2 = xz - y$, $f_3 = xy - z$. The term order $\prec_1$ is the Degree Reverse Lex order with $(x \succ y \succ z)$.*

For a polynomial $f = y^2 - z^2 \in I$, since $\{f_1, f_2, f_3\}$ is a set of generators of I, the polynomial f has a representation w.r.t. f_1, f_2, f_3:

$$f = 0 \cdot f_1 - y \cdot f_2 + z \cdot f_3 = (0, -y, z) \cdot (f_1, f_2, f_3),$$

where "$\cdot$" is the inner product of two vectors.

The vector (f_1, f_2, f_3) is fixed to the ideal I, so the polynomial f is determined by the vector $(0, -y, z)$. Let $\mathbf{u} := (0, -y, z) \in \mathbb{Q}[x, y, z]^3$. Then the vector $\mathbf{u}$ can be regard as an **ID** of f. Note that ID of $f = y^2 - z^2$ is not unique. For example, $\mathbf{u}' = (xz - y, -yz + x - y, z) \in \mathbb{Q}[x, y, z]^3$ is also an ID of this f.

In general case, for any $f \in I$, there always exists $\mathbf{u} = (p_1, p_2, p_3) \in R^3 = \mathbb{Q}[x, y, z]^3$, such that

$$f = \mathbf{u} \cdot (f_1, f_2, f_3) = p_1 \cdot f_1 + p_2 \cdot f_2 + p_3 \cdot f_3.$$

That is, any polynomial in I has at least one ID. To express the relation between f and $\mathbf{u}$, we use the notation $f^{[\mathbf{u}]}$, which means $f = \mathbf{u} \cdot (f_1, f_2, f_3)$. [2] For convenience, we also call $f^{[\mathbf{u}]}$ to be a polynomial in I. For example, $(y^2 - z^2)^{[-y\mathbf{e}_2 + z\mathbf{e}_3]}$ and $(y^2 - z^2)^{[(xz-y)\mathbf{e}_1 + (-yz+x-y)\mathbf{e}_2 + z\mathbf{e}_3]}$ are two polynomials in I, and *we treat* $(y^2 - z^2)^{[-y\mathbf{e}_2 + z\mathbf{e}_3]}$ *and* $(y^2 - z^2)^{[(xz-y)\mathbf{e}_1 + (-yz+x-y)\mathbf{e}_2 + z\mathbf{e}_3]}$ *as different polynomials in this paper*, i.e. $f^{[\mathbf{u}]} = f'^{[\mathbf{u}']}$ if and only if $f = f'$ and $\mathbf{u} = \mathbf{u}'$.

The computations on $f^{[\mathbf{u}]}$ can be defined naturally. Let $f^{[\mathbf{u}]}$ and $g^{[\mathbf{v}]}$ be two polynomials such that $f = \mathbf{u} \cdot (f_1, f_2, f_3)$ and $g = \mathbf{v} \cdot (f_1, f_2, f_3)$, c be a constant in $\mathbb{Q}$ and t be a power product in R. Then

1. $f^{[\mathbf{u}]} + g^{[\mathbf{v}]} = (f + g)^{[\mathbf{u}+\mathbf{v}]}$.
2. $ct(f^{[\mathbf{u}]}) = (ctf)^{[ct\mathbf{u}]}$.

Clearly, the operations are well defined, i.e. $f + g = (\mathbf{u} + \mathbf{v}) \cdot (f_1, f_2, f_3)$ and $ctf = (ct\mathbf{u}) \cdot (f_1, f_2, f_3)$.

Since $\mathbf{u}$ is a vector in the free module R^3, we consider a term order $\prec_2$ on R^3. The term order $\prec_2$ can be any admissible term order. In this example, we use the term order introduced in F5, i.e.

$$x^\alpha \mathbf{e}_i \prec_2 x^\beta \mathbf{e}_j \text{ iff } \begin{cases} i > j, \\ \text{ or} \\ i = j \text{ and } x^\alpha \prec_1 x^\beta, \end{cases}$$

where $\mathbf{e}_1 = (1, 0, 0)$, $\mathbf{e}_2 = (0, 1, 0)$ and $\mathbf{e}_3 = (0, 0, 1)$. When the term order on R^3 is fixed, we can define the *leading power product* and *leading coefficient* of $\mathbf{u} = (p_1, p_2, p_3) = p_1\mathbf{e}_1 + p_2\mathbf{e}_2 + p_3\mathbf{e}_3 \in R^3$ to be $\mathrm{lpp}(\mathbf{u})$ and $\mathrm{lc}(\mathbf{u})$ similarly. More related definitions on "module" can be found in Chapter 5 of (Cox et al., 2004).

Then for a polynomial $f^{[\mathbf{u}]}$ where $f = \mathbf{u} \cdot (f_1, f_2, f_3)$, we define $\mathrm{lpp}(\mathbf{u})$ to be the **signature** of $f^{[\mathbf{u}]}$. For example, the signature of $(y^2 - z^2)^{[-y\mathbf{e}_2 + z\mathbf{e}_3]}$ is $\mathrm{lpp}(-y\mathbf{e}_2 + z\mathbf{e}_3) = y\mathbf{e}_2$. Original definition of signature is introduced by Faugère in (Faugère, 2002), and recently, Gao et al. give a generalized definition of signature in (Gao et al., 2010b). In this paper, we use the generalized definition given by Gao et al.

With signatures, we can then compare polynomials in I w.r.t. their signatures. That is, we say $f^{[\mathbf{u}]}$ is *bigger* than $g^{[\mathbf{v}]}$, if $f^{[\mathbf{u}]}$ has bigger signature than $g^{[\mathbf{v}]}$, i.e. $\mathrm{lpp}(\mathbf{u}) \succ_2 \mathrm{lpp}(\mathbf{v})$.

[2] An equivalent notation $(\mathbf{u}, f)$ is used in (Sun and Wang, 2011). Now we prefer $f^{[\mathbf{u}]}$ to $(\mathbf{u}, f)$, since the notation $f^{[\mathbf{u}]}$ indicates $\mathbf{u}$ is only an auxiliary value to f.

Now we actually set up an *ordering* on the polynomials in I. Moreover, if we deal with the polynomials according to this ordering, we will have a very beautiful property, which is the key fact in next subsection.

2.3. Key fact

For a general ideal $I = \langle f_1, \cdots, f_m \rangle \subset R$, we find the following key fact.

Key Fact: *Let $f^{[\mathbf{u}]}$, $g^{[\mathbf{v}]}$ be two polynomials and G be a subset of I. Suppose $f^{[\mathbf{u}]}$ and $g^{[\mathbf{v}]}$ are reduced to $f'^{[\mathbf{u}']}$ and $g'^{[\mathbf{v}']}$ by G respectively. Then f' and g' have the same leading power product, i.e.* $\mathrm{lpp}(f') = \mathrm{lpp}(g')$, *if $f^{[\mathbf{u}]}$* ***and*** *$g^{[\mathbf{v}]}$* ***have the same signature****, i.e.* $\mathrm{lpp}(\mathbf{u}) = \mathrm{lpp}(\mathbf{v})$, *and two extra conditions hold.*

Briefly, Key Fact means that *reducing f and g could create the same leading power product if $f^{[\mathbf{u}]}$ and $g^{[\mathbf{v}]}$ have the same signature.* This fact is very interesting and important, from which we can predict the reducing result of polynomials without really reducing them, and hence we can answer the important question proposed in Subsection 2.1.

Next, let us see the two extra conditions. We emphasize the first condition.

Condition 1: *A* ***one-side-reduction****, which is defined below, must be used in Key Fact.*

Definition 2.2. *We say $f^{[\mathbf{u}]}$ is* ***reducible*** *by $h^{[\mathbf{w}]} \in G$, only if*

1. $\mathrm{lpp}(h)$ *divides* $\mathrm{lpp}(f)$, *and*
2. $t(h^{[\mathbf{w}]})$*'s signature* $\prec_2$ $f^{[\mathbf{u}]}$*'s signature, i.e.* $\mathrm{lpp}(t\mathbf{w}) \prec_2 \mathrm{lpp}(\mathbf{u})$ *where* $t = \mathrm{lpp}(f)/\mathrm{lpp}(h)$.

If $f^{[\mathbf{u}]}$ is reducible by $h^{[\mathbf{w}]} \in G$, then $f^{[\mathbf{u}]} \longmapsto_G f^{[\mathbf{u}]} - ct(h^{[\mathbf{w}]})$ is called a ***one-step-reduction*** *by G where $c = \mathrm{lc}(f)/\mathrm{lc}(h)$ and $t = \mathrm{lpp}(f)/\mathrm{lpp}(h)$.*

We say $f^{[\mathbf{u}]}$ ***is reduced to*** *$f'^{[\mathbf{u}']}$* ***by*** *G, if $f'^{[\mathbf{u}']}$ is obtained by several one-step-reductions from $f^{[\mathbf{u}]}$, and $f'^{[\mathbf{u}']}$ is not reducible by G.*

In simple words, this one-side-reduction indicates $f^{[\mathbf{u}]}$ *can only be reduced by polynomials having smaller signatures.* In Example 2.1, $(xyz - y^2)^{[y\mathbf{e}_2]}$ is *reducible* by $(xy - z)^{[\mathbf{e}_3]}$ but *not reducible* by $(yz - x)^{[\mathbf{e}_1]}$. The reason comes from the constraint of signatures.

Note that for the result $f^{[\mathbf{u}]} - ct(h^{[\mathbf{w}]}) = (f - cth)^{[\mathbf{u} - ct\mathbf{w}]}$ of the one-step-reduction, we still have $(\mathbf{u} - ct\mathbf{w}) \cdot (f_1, \cdots, f_m) = \mathbf{u} \cdot (f_1, \cdots, f_m) - ct\mathbf{w} \cdot (f_1, \cdots, f_m) = f - cth$. So for $f'^{[\mathbf{u}']}$, the equation $f' = \mathbf{u}' \cdot (f_1, \cdots, f_m)$ also holds. Moreover, if $f^{[\mathbf{u}]}$ is reduced to $f'^{[\mathbf{u}']}$, then $f^{[\mathbf{u}]}$ and $f'^{[\mathbf{u}']}$ must have the same signature, i.e. $\mathrm{lpp}(\mathbf{u}) = \mathrm{lpp}(\mathbf{u}')$.

Now we can see how the *ordering* on the polynomials is used in Key Fact. That is, if $f^{[\mathbf{u}]}$ and $g^{[\mathbf{v}]}$ have the same signature, and only the polynomials having smaller signatures are used to reduce $f^{[\mathbf{u}]}$ and $g^{[\mathbf{v}]}$, then the reducing results f' and g' could have the same leading power product.

Therefore, this one-side-reduction is a necessary condition to the key fact. We notice that *all existing signature-based algorithms are using this kind of one-side-reduction.*

Condition 2: *For any $\bar{f}^{[\bar{\mathbf{u}}]} \in I$ with $\bar{f}^{[\bar{\mathbf{u}}]}$'s signature $\prec_2$ $f^{[\mathbf{u}]}$'s signature, i.e.* $\mathrm{lpp}(\bar{\mathbf{u}}) \prec_2 \mathrm{lpp}(\mathbf{u})$, *there always exists $h^{[\mathbf{w}]} \in G$ such that*

1. $\mathrm{lpp}(h)$ *divides* $\mathrm{lpp}(\bar{\mathbf{u}})$, *and*
2. $t(h^{[\mathbf{w}]})$*'s signature* $\preceq_2$ $\bar{f}^{[\bar{\mathbf{u}}]}$*'s signature, i.e.* $\mathrm{lpp}(t\mathbf{w}) \preceq_2 \mathrm{lpp}(\bar{\mathbf{u}})$ *where* $t = \mathrm{lpp}(\bar{f})/\mathrm{lpp}(h)$.

The second condition may be a bit difficult to understand, but it is satisfied in all existing signature-based algorithms.

With Condition 1 and 2, we can prove Key Fact easily.

Proof of Key Fact. We prove it by contradiction.

Assume $\mathrm{lpp}(f') \succ \mathrm{lpp}(g')$. Since a one-side-reduction is used in Key Fact, we have $\mathrm{lpp}(\mathbf{u}') = \mathrm{lpp}(\mathbf{u}) = \mathrm{lpp}(\mathbf{v}) = \mathrm{lpp}(\mathbf{v}')$. Let $\bar{f}^{[\bar{\mathbf{u}}]} := f'^{[\mathbf{u}']} - c(g'^{[\mathbf{v}']})$ where $c = \mathrm{lc}(\mathbf{u}')/\mathrm{lc}(\mathbf{v}')$, then $\mathrm{lpp}(\bar{f}) = \mathrm{lpp}(f')$ and $\mathrm{lpp}(\bar{\mathbf{u}}) \prec_2 \mathrm{lpp}(\mathbf{u}') = \mathrm{lpp}(\mathbf{u})$. By Condition 2, there exists $h^{[\mathbf{w}]} \in G$ such that $\mathrm{lpp}(h)$ divides $\mathrm{lpp}(\bar{f}) = \mathrm{lpp}(f')$ and $\mathrm{lpp}(t\mathbf{w}) \preceq_2 \mathrm{lpp}(\bar{\mathbf{u}}) \prec_2 \mathrm{lpp}(\mathbf{u}')$ where $t = \mathrm{lpp}(\bar{f})/\mathrm{lpp}(h)$. This means $f'^{[\mathbf{u}']}$ is still reducible by $h^{[\mathbf{w}]} \in G$, which contracts with the definition of one-side-reduction.

The case $\mathrm{lpp}(f') \prec \mathrm{lpp}(g')$ can be proved similarly. □

2.4. Observations

Using Key Fact, we get the following important observations.

Observations 1: *If* $f^{[\mathbf{u}]}$ *and* $g^{[\mathbf{v}]}$ *have the same signature, then at most one of them is necessary to be reduced.*

Observations 2: *Particularly, if* $f^{[\mathbf{u}]}$ *and* $g^{[\mathbf{v}]}$ *have the same signature and either* $f = 0$ *or* $g = 0$*, then neither one is necessary to be reduced.*

We notice that all existing criteria are based on the above two observations. These observations also motivate the generalized criterion for signature-based algorithms.

3. Generalized Criterion

3.1. Generalized criterion

Let $R := \mathrm{K}[x_1, \cdots, x_n]$ and $\mathbf{f} := (f_1, \cdots, f_m) \in R^m$. In the rest of paper, we consider the following ideal

$$I := \langle f_1, \cdots, f_m \rangle = \{\mathbf{u} \cdot \mathbf{f} = p_1 f_1 + \cdots + p_m f_m \mid \mathbf{u} = (p_1, \cdots, p_m) \in R^m\}$$

with respect to some term order on R. The notation $f^{[\mathbf{u}]}$ always means $f = \mathbf{u} \cdot \mathbf{f}$, and for convenience, we also call $f^{[\mathbf{u}]}$ to be a polynomial in I and write $f^{[\mathbf{u}]} \in I$. Let $\mathbf{e}_i$ be the i-th unit vector of R^m, i.e. $(\mathbf{e}_i)_j = \delta_{ij}$ where δ_{ij} is the Kronecker delta. Then $f_1^{[\mathbf{e}_1]}, \cdots, f_m^{[\mathbf{e}_m]}$ are polynomials in I. Note that if there exists $\mathbf{u}' \neq \mathbf{u}$ such that $f = \mathbf{u}' \cdot \mathbf{f}$, then $f^{[\mathbf{u}]}$ and $f^{[\mathbf{u}']}$ are treated as two different polynomials in I.

Fix *any* term order $\prec_1$ on R and *any* term order $\prec_2$ on R^m. We must emphasize that the order $\prec_2$ may or may not be related to $\prec_1$ in theory, although $\prec_2$ is usually an extension of $\prec_1$ to R^m in implementation. For sake of convenience, we use $\prec$ to represent $\prec_1$ and $\prec_2$, if no confusion occurs. We make the convention that if $f = 0$ then $\mathrm{lpp}(f) = 0$ and $0 \prec t$ for any non-zero power product t in R; similarly for $\mathrm{lpp}(\mathbf{u})$.

Given a finite set $B \subset I$, consider a **partial order** "$<$" defined on B, where "$<$" has:

1. Non-Reflexivity: $f^{[\mathbf{u}]} \not< f^{[\mathbf{u}]}$ for all $f^{[\mathbf{u}]} \in B$.
2. Antisymmetry: $f^{[\mathbf{u}]} < g^{[\mathbf{v}]}$ does not imply $g^{[\mathbf{v}]} < f^{[\mathbf{u}]}$, where $f^{[\mathbf{u}]}, g^{[\mathbf{v}]} \in B$.
3. Transitivity: $f^{[\mathbf{u}]} < g^{[\mathbf{v}]}$ and $g^{[\mathbf{v}]} < h^{[\mathbf{w}]}$ imply $f^{[\mathbf{u}]} < h^{[\mathbf{w}]}$, where $f^{[\mathbf{u}]}, g^{[\mathbf{v}]}, h^{[\mathbf{w}]} \in B$.

Now we give a generalized criterion for signature-based algorithms.

Definition 3.1 (generalized rewritable criterion)**.** *Let B be a subset of I, "$<$" be a partial order on B, $f^{[\mathbf{u}]}$ be a polynomial in B and t be a power product in R where $f \neq 0$. We say $t(f^{[\mathbf{u}]})$ is* **generalized rewritable** *by B (***gen-rewritable** *for short), if there exists $g^{[\mathbf{v}]} \in B$ such that*

1. $\mathrm{lpp}(\mathbf{v})$ *divides* $\mathrm{lpp}(t\mathbf{u})$*, and*
2. $g^{[\mathbf{v}]} < f^{[\mathbf{u}]}$.

If $t(f^{[\mathbf{u}]})$ is gen-rewritable by $g^{[\mathbf{v}]} \in B$, then $\mathrm{lpp}(\mathbf{v})$ divides $\mathrm{lpp}(t\mathbf{u})$. Let $t' := \mathrm{lpp}(t\mathbf{u})/\mathrm{lpp}(\mathbf{v})$. Note that $t(f^{[\mathbf{u}]})$ and $t'(g^{[\mathbf{v}]})$ have the same signature, i.e. $\mathrm{lpp}(t\mathbf{u}) = \mathrm{lpp}(t'\mathbf{v})$, so according to Observation 1, at most one of $t(f^{[\mathbf{u}]})$ and $t'(g^{[\mathbf{v}]})$ is necessary to be reduced during the computations. The partial order "$<$" on B will help to choose the polynomial that is not to be reduced, and in the above definition, the "bigger" polynomial under the partial order is selected. So in practice, if $t(f^{[\mathbf{u}]})$ is gen-rewritable by B, then $t(f^{[\mathbf{u}]})$ will not be reduced.

Generally, the partial order on B can be defined in many ways. For example, since the set B is usually the intermediate set of generators and polynomials in B are often added one by one, then we can define "$<$" as: $g^{[\mathbf{v}]} < f^{[\mathbf{u}]}$, if $g^{[\mathbf{v}]}$ is added to B later than $f^{[\mathbf{u}]}$. There are two other partial orders: $g^{[\mathbf{v}]} < f^{[\mathbf{u}]}$ if $\mathrm{lpp}(g) < \mathrm{lpp}(f)$, or even $g^{[\mathbf{v}]} < f^{[\mathbf{u}]}$ if f has more terms than g. All of these partial orders can be used in the above definition, but as we will see later, *not all partial orders lead to correct criterion.*

Observation 2 says if $f^{[\mathbf{u}]}$ and $g^{[\mathbf{v}]}$ have the same signature and either $f = 0$ or $g = 0$, then neither $f^{[\mathbf{u}]}$ nor $g^{[\mathbf{v}]}$ is necessary to be reduced. In fact, $0^{[\mathbf{u}]}$ means $\mathbf{u}$ is a syzygy of $\mathbf{f} = (f_1, \cdots, f_m)$, i.e. $\mathbf{u} \cdot \mathbf{f} = 0$. For convenience, we call the polynomial $0^{[\mathbf{u}]}$ to be **syzygy polynomial**. By using syzygy polynomials, the generalized criterion can be enhanced. That is, we can add syzygy polynomials to the set B and assume syzygy polynomials are "smaller" than other polynomials under the partial order, then more redundant computations can be rejected. This technique is used in the algorithm AGC in next subsection.

The following proposition shows many syzygy polynomials can be obtained directly.

Proposition 3.2. *Let $f^{[\mathbf{u}]}$ be a polynomial in I. Then $0^{[f\mathbf{e}_i - f_i\mathbf{u}]}$ is a syzygy polynomial where $1 \leq i \leq m$.*

Proof. Since $f = \mathbf{u} \cdot (f_1, \cdots, f_m)$, then

$$(f\mathbf{e}_i - f_i\mathbf{u}) \cdot (f_1, \cdots, f_m) = f\mathbf{e}_i \cdot (f_1, \cdots, f_m) - f_i\mathbf{u} \cdot (f_1, \cdots, f_m) = ff_i - f_if = 0.$$

□

Since the syzygy polynomial $0^{[f\mathbf{e}_i - f_i\mathbf{u}]}$ in Proposition 3.2 uses the principal syzygy of f and f_i, we call syzygy polynomials in form of $0^{[f\mathbf{e}_i - f_i\mathbf{u}]}$ to be **principle syzygy polynomials**.

In Section 4, we will show how the generalized criterion specializes to F5 and GVW's criteria. Next, we describe how this generalized criterion is used in algorithm.

3.2. How the generalized criterion is used?

We first define the *critical pairs* of two polynomials. Suppose $f^{[\mathbf{u}]}, g^{[\mathbf{v}]}$ are two polynomials with f and g both nonzero. Let $t := \mathrm{lcm}(\mathrm{lpp}(f), \mathrm{lpp}(g))$, $t_f := t/\mathrm{lpp}(f)$ and $t_g := t/\mathrm{lpp}(g)$. If $t_f(f^{[\mathbf{u}]})$'s signature $\succeq$ $t_g(g^{[\mathbf{v}]})$'s signature, i.e. $\mathrm{lpp}(t_f\mathbf{u}) \succeq \mathrm{lpp}(t_g\mathbf{v})$, then the following 4-tuple vector

$$(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$$

is called the **critical pair** of $f^{[\mathbf{u}]}$ and $g^{[\mathbf{v}]}$. The corresponding **S-polynomial** is $t_f(f^{[\mathbf{u}]}) - ct_g(g^{[\mathbf{v}]})$ where $c = \mathrm{lc}(f)/\mathrm{lc}(g)$. Please keep in mind that, for any critical pair $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$, we always have $t_f(f^{[\mathbf{u}]})$'s signature $\succeq$ $t_g(g^{[\mathbf{v}]})$'s signature, i.e. $\mathrm{lpp}(t_f\mathbf{u}) \succeq \mathrm{lpp}(t_g\mathbf{v})$. Also note that t_f (or t_g) here does not mean it only depends on f (or g). For convenience, the critical pair of $f^{[\mathbf{u}]}$ and $g^{[\mathbf{v}]}$ is also denoted as $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ or $[g^{[\mathbf{v}]}, f^{[\mathbf{u}]}]$ for short, and we say $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ is a critical pair of B, if both $f^{[\mathbf{u}]}$ and $g^{[\mathbf{v}]}$ are in B.

Critical pairs can be classed in three kinds. Let $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ be a critical pair and $t_f(f^{[\mathbf{u}]}) - ct_g(g^{[\mathbf{v}]})$ be its S-polynomial where $c = \mathrm{lc}(f)/\mathrm{lc}(g)$.

1. If $t_f(f^{[\mathbf{u}]}) - ct_g(g^{[\mathbf{v}]})$'s signature $\prec$ $t_f(f^{[\mathbf{u}]})$'s signature, i.e. $\mathrm{lpp}(t_f\mathbf{u} - ct_g\mathbf{v}) \neq \mathrm{lpp}(t_f\mathbf{u})$, then we say $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is **non-regular**.
2. If $t_f(f^{[\mathbf{u}]}) - ct_g(g^{[\mathbf{v}]})$, $t_f(f^{[\mathbf{u}]})$ and $t_g(g^{[\mathbf{v}]})$ have the same signature, i.e. $\mathrm{lpp}(t_f\mathbf{u} - ct_g\mathbf{v}) = \mathrm{lpp}(t_f\mathbf{u}) = \mathrm{lpp}(t_g\mathbf{v})$, then $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is called **super regular**.
3. If $t_f(f^{[\mathbf{u}]})$'s signature $\succ$ $t_g(g^{[\mathbf{v}]})$'s signature, i.e. $\mathrm{lpp}(t_f\mathbf{u}) \succ \mathrm{lpp}(t_g\mathbf{v})$, then we call $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ to be **regular**.

We say a **critical pair** $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ **is gen-rewritable by a set** B, if *either* $t_f(f^{[\mathbf{u}]})$ *or* $t_g(g^{[\mathbf{v}]})$ is gen-rewritable by B.

Then the generalized criterion is used in the following way:

A critical pair $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ *of* B *is* ***rejected by the generalized criterion****, if*

1. *it is not regular, i.e.* $\mathrm{lpp}(t_f\mathbf{u}) = \mathrm{lpp}(t_g\mathbf{v})$*, or*
2. *it is regular and generalized rewritable by* B*, i.e.* $\mathrm{lpp}(t_f\mathbf{u}) \succ \mathrm{lpp}(t_g\mathbf{v})$*, and either* $t_f(f^{[\mathbf{u}]})$ *or* $t_g(g^{[\mathbf{v}]})$ *is generalized rewritable by* B*.*

If a critical pair is rejected by the generalized criterion, then this critical pair will not be considered in algorithm. We can also show how the generalized criterion is used through a simple algorithm(Algorithm 1).

For the above algorithm, please note that

1. The gen-rewritable criterion uses a partial order defined on G. While new elements are added to G, the partial order on G needs to be updated simultaneously. Fortunately, most partial orders can be updated automatically.
2. For the line ended with ($\bigstar$), we emphasize that any critical pair can be selected, while some other algorithm, such as GVW, always selects the critical pair with minimal signature.
3. *Principle syzygy polynomials* are added to G at lines marked with ($\Diamond$).

Algorithm 1: The algorithm with generalized criterion (AGC)

Input : $f_1^{[\mathbf{e}_1]}, \cdots, f_m^{[\mathbf{e}_m]}$.
Output: A subset $G \subset \langle f_1, \cdots, f_m \rangle$.
begin
  $G \longleftarrow \{f_i^{[\mathbf{e}_i]} \mid i = 1, \cdots, m\} \cup \{0^{[f_j \mathbf{e}_i - f_i \mathbf{e}_j]} \mid 1 \leq i < j \leq m\}$ $(\Diamond)$
  $CPairs \longleftarrow \{[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}] \mid f^{[\mathbf{u}]}, g^{[\mathbf{v}]} \in G\}$
  while $CPairs \neq \emptyset$ **do**
    $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}] = (t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]}) \longleftarrow$ **any** critical pair in $CPairs$ $(\bigstar)$
    $CPairs \longleftarrow CPairs \setminus \{[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]\}$
    if $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ *is* **regular** *and is* **not gen-rewritable** *by* G **then**
      $h^{[\mathbf{w}]} \longleftarrow$ reduce the S-polynomial of $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ by G
      $CPairs \longleftarrow CPairs \cup \{[h^{[\mathbf{w}]}, g^{[\mathbf{v}]}] \mid g^{[\mathbf{v}]} \in G\}$
      $G \longleftarrow G \cup \{h^{[\mathbf{w}]}\} \cup \{0^{[h\mathbf{e}_i - f_i \mathbf{w}]} \mid i = 1, \cdots, m\}$ $(\Diamond)$
    end if
  end
  return G
end

4. The S-polynomial of $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ is reduced by the one-side-reduction defined in Definition 2.2. Note that for the reducing result $h^{[\mathbf{w}]}$, we still have $h = \mathbf{w} \cdot (f_1, \cdots, f_m)$. Other similar one-side-reductions in (Gao et al., 2010b; Hashemi and Ars, 2010; Faugère, 2002) can also be used here.
5. The S-polynomial of $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is considered only when $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is *regular*, so its S-polynomial $t_f(f^{[\mathbf{u}]}) - ct_g(g^{[\mathbf{v}]})$ and $t_f(f^{[\mathbf{u}]})$ have the same signature where $c = \mathrm{lc}(f)/\mathrm{lc}(g)$. Besides, the one-side-reduction does not affect the signatures, i.e. $t_f(f^{[\mathbf{u}]})$ and $h^{[\mathbf{w}]}$ also have the same signature. Therefore, for sake of efficiency, it suffices to record f and $\mathrm{lpp}(\mathbf{u})$ for each $f^{[\mathbf{u}]} \in G$ in the practical implementation, which is just the same as that F5 does.

The algorithm AGC aims to compute a Gröbner basis for $\langle f_1, \cdots, f_m \rangle$. However, the generalized criterion may reject useful critical pairs sometimes, which makes the output of the algorithm AGC is not a Gröbner basis. In next subsection, we will show when the generalized criterion is correct, or equivalently, when the algorithm AGC outputs a Gröbner basis.

3.3. When the generalized criterion is correct?

In fact, the algorithm AGC can construct a even "stronger" version of Gröbner basis. Let

$$G := \{g_1^{[\mathbf{v}_1]}, \cdots, g_s^{[\mathbf{v}_s]}\}$$

be a finite subset of I. We call G a **labeled Gröbner basis**[3] for I, if for any $f^{[\mathbf{u}]} \in I$ with $f \neq 0$, there exists $g^{[\mathbf{v}]} \in G$ such that

1. $\mathrm{lpp}(g)$ divides $\mathrm{lpp}(f)$, and
2. $t(g^{[\mathbf{v}]})$'s signature $\preceq f^{[\mathbf{u}]}$'s signature, i.e. $\mathrm{lpp}(t\mathbf{v}) \preceq \mathrm{lpp}(\mathbf{u})$, where $t = \mathrm{lpp}(f)/\mathrm{lpp}(g)$.

Proposition 3.3. *If G is a labeled Gröbner basis for I, then the set $\{g \mid g^{[\mathbf{v}]} \in G\}$ is a Gröbner basis of the ideal $I = \langle f_1, \cdots, f_m \rangle$.*

Proof. For any $f \in \langle f_1, \cdots, f_m \rangle$, there exist $p_1, \cdots, p_m \in R$ such that $f = p_1 f_1 + \cdots + p_m f_m$. Let $\mathbf{u} := (p_1, \cdots, p_m)$. Then $f^{[\mathbf{u}]} \in I$ and hence there exists $g^{[\mathbf{v}]} \in G$ such that $\mathrm{lpp}(g)$ divides $\mathrm{lpp}(f)$ by the definition of labeled Gröbner basis. □

The algorithm AGC outputs a labeled Gröbner basis for I, if the partial order in the generalized criterion is *admissible*. In the algorithm AGC, we say a partial order "$<$" is **admissible**, if for any critical pair $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ of G, whenever we need to reduce the S-polynomial of $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ to $h^{[\mathbf{w}]}$ by G, we always have $h^{[\mathbf{w}]} < f^{[\mathbf{u}]}$ after updating "$<$" for $G \cup \{h^{[\mathbf{w}]}\}$. In next section, we will show that the partial orders implied by F5 and GVW's criteria are both admissible.

Note that only the critical pair *that is regular and not gen-rewritable* is really reduced in the algorithm AGC, so when checking whether a partial order is admissible, we do not care about the critical pairs that are rejected by the generalized criterion. Besides, we emphasize that in the above definition of admissible, the relation $h^{[\mathbf{w}]} < f^{[\mathbf{u}]}$ is essential, and $h^{[\mathbf{w}]}$ may not be related to other elements in G.

The following theorem shows when the generalized criterion is correct in the algorithm AGC. The proof of theorem will be presented in Section 5.

Theorem 3.4. *Let $I := \langle f_1, \cdots, f_m \rangle$ be an ideal in R. Then a labeled Gröbner basis for I can be constructed by the algorithm AGC, if the algorithm AGC terminates in finite steps and the partial order in the generalized criterion is admissible.*

4. Specializations

In this section, we focus on specializing the generalized criterion to F5 and GVW's criteria by using appropriate admissible partial orders. By saying "specialize", we mean the critical pairs rejected by F5 or GVW's criteria can also be rejected by the generalized criterion.

[3] Labeled Gröbner basis is exactly the same as the S-Gröbner basis in (Sun and Wang, 2011), and it is also a simpler version of *strong Gröbner basis* defined in (Gao et al., 2010b), so the GVW algorithm computes a labeled Gröbner basis. We proved in another paper that F5 also computes a labeled Gröbner basis.

4.1. F5's criteria

First, we list the F5's criteria with current notations. In F5, the order $\prec_2$ on R^m is obtained by extending $\prec_1$ to R^m in a *position over term* fashion, i.e.

$$x^\alpha \mathbf{e}_i \prec_2 x^\beta \mathbf{e}_j \text{ iff } \begin{cases} i > j, \\ \text{ or} \\ i = j \text{ and } x^\alpha \prec_1 x^\beta. \end{cases}$$

This term order makes F5 work incrementally.

Definition 4.1 (syzygy criterion)**.** *Let B be a subset of I, $f^{[\mathbf{u}]}$ be a polynomial in B and t be a power product in R where $f \neq 0$ and $\mathrm{lpp}(\mathbf{u}) = x^\alpha \mathbf{e}_i$. We say $t(f^{[\mathbf{u}]})$ is* **F5-divisible** *by B, if there exists $g^{[\mathbf{v}]} \in B$ with $\mathrm{lpp}(\mathbf{v}) = x^\beta \mathbf{e}_j$, such that*

1. $\mathrm{lpp}(g)$ *divides* tx^α*, and*
2. $\mathbf{e}_i \succ \mathbf{e}_j$*.*

Definition 4.2 (rewritten criterion)**.** *Let B be a subset of I, $f^{[\mathbf{u}]}$ be a polynomial in B and t be a power product in R. We say $t(f^{[\mathbf{u}]})$ is* **F5-rewritable** *by B, if there exists $g^{[\mathbf{v}]} \in B$, such that*

1. $\mathrm{lpp}(\mathbf{v})$ *divides* $\mathrm{lpp}(t\mathbf{u})$*, and*
2. $g^{[\mathbf{v}]}$ *is added to B later than $f^{[\mathbf{u}]}$.*

In F5, a critical pair $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ of B is rejected by the syzygy criterion or rewritten criterion if either $t_f(f^{[\mathbf{u}]})$ or $t_g(g^{[\mathbf{v}]})$ is F5-divisible or F5-rewritable by B.

Next, we show how the generalized criterion specializes to both syzygy criterion and rewritten criterion at the same time. For this purpose, the following partial order on G, which can be updated automatically when a new element is added to G, is used: For any $f^{[\mathbf{u}]}, g^{[\mathbf{v}]} \in G$, we say $g^{[\mathbf{v}]} < f^{[\mathbf{u}]}$ if

1. $f \neq 0$ and $g^{[\mathbf{v}]} = 0^{[\mathbf{v}]}$ is a *principle syzygy polynomial*,
2. otherwise, $g^{[\mathbf{v}]}$ is added to G later than $f^{[\mathbf{u}]}$.

The above partial order "$<$" is *admissible* in the algorithm AGC. Because for any critical pair $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ of G, when we need to reduce its S-polynomial to $h^{[\mathbf{w}]}$ by G, the polynomial $h^{[\mathbf{w}]}$ is always added to G later than $f^{[\mathbf{u}]}$ no matter h is 0 or not, since $f^{[\mathbf{u}]}$ is already in G.

At last, we show how the generalized criterion specializes to the rewritten criterion and syzygy criterion. For the rewritten criterion, the specialization is obvious by the definition of "$<$". For the syzygy criterion, if $t(f^{[\mathbf{u}]})$, where $f^{[\mathbf{u}]} \in G$ with $\mathrm{lpp}(\mathbf{u}) = x^\alpha \mathbf{e}_i$ and $f \neq 0$, is F5-divisible by some $g^{[\mathbf{v}]} \in G$ with $\mathrm{lpp}(\mathbf{v}) = x^\beta \mathbf{e}_j$, we have $\mathrm{lpp}(g)$ divides tx^α and $\mathbf{e}_i \succ \mathbf{e}_j$. Since $g^{[\mathbf{v}]} \in G$, ccording to the algorithm AGC, the principle syzygy polynomial $0^{[g\mathbf{e}_i - f_i\mathbf{v}]}$ has been added to G, and $\mathrm{lpp}(g\mathbf{e}_i - f_i\mathbf{v}) = \mathrm{lpp}(g)\mathbf{e}_i$ divides $tx^\alpha \mathbf{e}_i$. So $t(f^{[\mathbf{u}]})$ is gen-rewritable by $0^{[g\mathbf{e}_i - f_i\mathbf{v}]} \in G$. Therefore, the critical pairs rejected by F5's criteria can also be rejected by the generalized criterion.

With a similar discussion, the generalized criterion can also specialize to the criteria in (Hashemi and Ars, 2010), since the extended F5 algorithm in that paper only differs from the original F5 in the order $\prec_2$ on R^m.

4.2. GVW's Criteria

First, we rewrite the GVW's criteria with current notations.

Definition 4.3 (First Criterion)**.** *Let B be a subset of I, $f^{[\mathbf{u}]}$ be a polynomial in B and t be a power product in R where $f \neq 0$. We say $t(f^{[\mathbf{u}]})$ is* **GVW-divisible** *by B, if there exists $g^{[\mathbf{v}]} \in B$ such that*

1. $\mathrm{lpp}(\mathbf{v})$ *divides* $\mathrm{lpp}(t\mathbf{u})$*, and*
2. $g = 0$.

Definition 4.4 (Second Criterion)**.** *Let B be a subset of I, $f^{[\mathbf{u}]}$ be a polynomial in B and t be a power product in R. We say $t(f^{[\mathbf{u}]})$ is* **eventually super top-reducible** *by B, if $t(f^{[\mathbf{u}]})$ is reducible and can be reduced to $h^{[\mathbf{w}]}$ by B, and there exists $g^{[\mathbf{v}]} \in B$ such that*

1. $\mathrm{lpp}(\mathbf{v})$ *divides* $\mathrm{lpp}(\mathbf{w})$*,*
2. $\mathrm{lpp}(g)$ *divides* $\mathrm{lpp}(h)$*, and*
3. $\frac{\mathrm{lpp}(\mathbf{w})}{\mathrm{lpp}(\mathbf{v})} = \frac{\mathrm{lpp}(h)}{\mathrm{lpp}(g)}$ *and* $\frac{\mathrm{lc}(\mathbf{w})}{\mathrm{lc}(\mathbf{v})} = \frac{\mathrm{lc}(h)}{\mathrm{lc}(g)}$.

In GVW, a critical pair $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ of B is rejected, if $t_f(f^{[\mathbf{u}]})$ is GVW-divisible or eventually super top-reducible by B. The GVW algorithm also has a third criterion.

Third Criterion *If there are two critical pairs $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ and $(t_{\bar{f}}, \bar{f}^{[\bar{\mathbf{u}}]}, t_{\bar{g}}, \bar{g}^{[\bar{\mathbf{v}}]})$ of B such that $t_f(f^{[\mathbf{u}]})$ and $t_{\bar{f}}(\bar{f}^{[\bar{\mathbf{u}}]})$ have the same signature, i.e. $\mathrm{lpp}(t_f\mathbf{u}) = \mathrm{lpp}(t_{\bar{f}}\bar{\mathbf{u}})$, then at least one of the two critical pairs is redundant.*

Next, in order to specialize the generalized criterion to the above three criteria at the same time, the following partial order on G, which can also be updated automatically when a new element is added to G, is used: for any $f^{[\mathbf{u}]}, g^{[\mathbf{v}]} \in G$, we say $g^{[\mathbf{v}]} < f^{[\mathbf{u}]}$ if one of the following two conditions holds:

1. $\mathrm{lpp}(t'g) < \mathrm{lpp}(tf)$, where $t' = \frac{\mathrm{lcm}(\mathrm{lpp}(\mathbf{u}),\mathrm{lpp}(\mathbf{v}))}{\mathrm{lpp}(\mathbf{v})}$ and $t = \frac{\mathrm{lcm}(\mathrm{lpp}(\mathbf{u}),\mathrm{lpp}(\mathbf{v}))}{\mathrm{lpp}(\mathbf{u})}$ such that $t(f^{[\mathbf{u}]})$ and $t'(g^{[\mathbf{v}]})$ have the same signature, i.e. $\mathrm{lpp}(t\mathbf{u}) = \mathrm{lpp}(t'\mathbf{v})$.
2. $\mathrm{lpp}(t'g) = \mathrm{lpp}(tf)$ and $g^{[\mathbf{v}]}$ is added to G later than $f^{[\mathbf{u}]}$.

The above partial order "$<$" is *admissible* in the algorithm AGC. Because for any critical pair $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ of G, when we need to reduce its S-polynomial to $h^{[\mathbf{w}]}$ by G, we always have $\mathrm{lpp}(t_f\mathbf{u}) = \mathrm{lpp}(\mathbf{w})$ and $\mathrm{lpp}(t_f f) > \mathrm{lpp}(h)$.

At last, let us see the three criteria of GVW.

For the first criterion, if $t(f^{[\mathbf{u}]})$ is GVW-divisible by some $g^{[\mathbf{v}]} \in G$, then $t(f^{[\mathbf{u}]})$ is also gen-rewritable by $g^{[\mathbf{v}]} \in G$ by definition.

For the second criterion, if $t(f^{[\mathbf{u}]})$, where $f^{[\mathbf{u}]} \in G$, is eventually super top-reducible by G, then $t(f^{[\mathbf{u}]})$ can be reduced to $h^{[\mathbf{w}]}$ and there exists $g^{[\mathbf{v}]} \in G$ such that $\mathrm{lpp}(\mathbf{v})$ divides $\mathrm{lpp}(\mathbf{w})$, $\mathrm{lpp}(g)$ divides $\mathrm{lpp}(h)$, $\frac{\mathrm{lpp}(\mathbf{w})}{\mathrm{lpp}(\mathbf{v})} = \frac{\mathrm{lpp}(h)}{\mathrm{lpp}(g)}$ and $\frac{\mathrm{lc}(\mathbf{w})}{\mathrm{lc}(\mathbf{v})} = \frac{\mathrm{lc}(h)}{\mathrm{lc}(g)}$. Then we have $\mathrm{lpp}(t'g) = \mathrm{lpp}(h) < \mathrm{lpp}(tf)$ and $\mathrm{lpp}(t'\mathbf{v}) = \mathrm{lpp}(\mathbf{w}) = \mathrm{lpp}(t\mathbf{u})$, which means $g^{[\mathbf{v}]} < f^{[\mathbf{u}]}$. So $t(f^{[\mathbf{u}]})$ is gen-rewritable by $g^{[\mathbf{v}]} \in G$.

For the third criterion, we have $\mathrm{lpp}(t_f\mathbf{u}) = \mathrm{lpp}(t_{\bar{f}}\bar{\mathbf{u}})$. Note that the above partial order is in fact a total order. First, if $f^{[\mathbf{u}]} < \bar{f}^{[\bar{\mathbf{u}}]}$, then $t_{\bar{f}}(\bar{f}^{[\bar{\mathbf{u}}]})$ is gen-rewritable by $f^{[\mathbf{u}]}$ and hence $(t_{\bar{f}}, \bar{f}^{[\bar{\mathbf{u}}]}, t_{\bar{g}}, \bar{g}^{[\bar{\mathbf{v}}]})$ is rejected; the reverse is also true. Second, if $f^{[\mathbf{u}]} = \bar{f}^{[\bar{\mathbf{u}}]}$, then one of the two critical pairs should be selected earlier from the set $CPairs$, assuming $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is selected first. On one hand, if $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is regular and not gen-rewritable, then its S-polynomial is reduced to $h^{[\mathbf{w}]}$ and $h^{[\mathbf{w}]}$ is added to G by the algorithm AGC. Since "$<$" is admissible, we have $h^{[\mathbf{w}]} < f^{[\mathbf{u}]}$. Thus, when the critical pair $(t_{\bar{f}}, \bar{f}^{[\bar{\mathbf{u}}]}, t_{\bar{g}}, \bar{g}^{[\bar{\mathbf{v}}]})$ is selected afterwards, it will be rejected, since $t_{\bar{f}}(\bar{f}^{[\bar{\mathbf{u}}]})$ is gen-rewritable by $h^{[\mathbf{w}]}$. On the other hand, if $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is not regular, or it is regular and gen-rewritable, then $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is rejected at once. Anyway, at least one of the two critical pairs is rejected in the algorithm.

5. Proofs for the Correctness of the Generalized Criterion

To prove Theorem 3.4, we need the following definition and lemmas.

In this section, we always assume that I is the ideal generated by $\{f_1, \cdots, f_m\}$. Let $f^{[\mathbf{u}]} \in I$, we say $f^{[\mathbf{u}]}$ has a **standard representation** w.r.t. a set $B \subset I$, if there exist $p_1, \cdots, p_s \in R$ and $g_1^{[\mathbf{v}_1]}, \cdots, g_s^{[\mathbf{v}_s]} \in B$ such that

$$f = p_1 g_1 + \cdots + p_s g_s,$$

where $\mathrm{lpp}(f) \succeq \mathrm{lpp}(p_i g_i)$ and $f^{[\mathbf{u}]}$'s signature $\succeq p_i(g_i^{[\mathbf{v}_i]})$'s signature, i.e. $\mathrm{lpp}(\mathbf{u}) \succeq \mathrm{lpp}(p_i\mathbf{v}_i)$ for $i = 1, \cdots, s$. Clearly, if $f^{[\mathbf{u}]}$ has a standard representation w.r.t. B, then there exists $g^{[\mathbf{v}]} \in B$ such that $\mathrm{lpp}(g)$ divides $\mathrm{lpp}(f)$ and $\mathrm{lpp}(\mathbf{u}) \succeq \mathrm{lpp}(t\mathbf{v})$ where $t = \mathrm{lpp}(f)/\mathrm{lpp}(g)$. We call this property to be the **basic property** of standard representations.

Lemma 5.1. *Let G be a finite subset of I and $\{f_1^{[\mathbf{e}_1]}, \cdots, f_m^{[\mathbf{e}_m]}\} \subset G$. For a polynomial $f^{[\mathbf{u}]} \in I$, $f^{[\mathbf{u}]}$ has a standard representation w.r.t. G, if for any critical pair $[g^{[\mathbf{v}]}, h^{[\mathbf{w}]}] = (t_g, g^{[\mathbf{v}]}, t_h, h^{[\mathbf{w}]})$ of G with $f^{[\mathbf{u}]}$'s signature $\succeq t_g(g^{[\mathbf{v}]})$'s signature, i.e. $\mathrm{lpp}(\mathbf{u}) \succeq \mathrm{lpp}(t_g\mathbf{v})$, the S-polynomial of $[g^{[\mathbf{v}]}, h^{[\mathbf{w}]}]$ always has a standard representation w.r.t. G.*

Proof. For $f^{[\mathbf{u}]} \in I$, we have $\mathbf{u} \cdot \mathbf{f} = f$ where $\mathbf{f} = (f_1, \cdots, f_m) \in R^m$. Assume $\mathbf{u} = p_1\mathbf{e}_1 + \cdots + p_m\mathbf{e}_m$ where $p_i \in R$. Clearly, $f = p_1 f_1 + \cdots + p_m f_m$. Note that $\mathrm{lpp}(\mathbf{u}) \succeq \mathrm{lpp}(p_i\mathbf{e}_i)$ for $i = 1, \cdots, m$. If $\mathrm{lpp}(f) \succeq \mathrm{lpp}(p_i f_i)$, then we have already got a standard representation for $f^{[\mathbf{u}]}$ w.r.t. G. Otherwise, we will prove it through classical method. Let $T := \max\{\mathrm{lpp}(p_i f_i) \mid i = 1, \cdots, m\}$, then $T \succ \mathrm{lpp}(f)$ holds by assumption. Consider the equation

$$f = \sum_{\mathrm{lpp}(p_i f_i) = T} \mathrm{lc}(p_i)\mathrm{lpp}(p_i) f_i + \sum_{\mathrm{lpp}(p_j f_j) \prec T} p_j f_j + \sum_{\mathrm{lpp}(p_i f_i) = T} (p_i - \mathrm{lc}(p_i)\mathrm{lpp}(p_i)) f_i. \qquad (1)$$

The leading power products in the first sum should be canceled, since we have $T \succ \mathrm{lpp}(f)$. So the first sum can be rewritten as a sum of S-polynomials, that is

$$\sum_{\mathrm{lpp}(p_i f_i) = T} \mathrm{lc}(p_i)\mathrm{lpp}(p_i) f_i = \sum \bar{c}t(t_g g - c t_h h),$$

where $g^{[\mathbf{v}]}, h^{[\mathbf{w}]} \in G$, $\bar{c} \in \mathrm{K}$, $t_g(g^{[\mathbf{v}]}) - ct_h(h^{[\mathbf{w}]})$ is the S-polynomial of $(t_g, g^{[\mathbf{v}]}, t_h, h^{[\mathbf{w}]})$, $\mathrm{lpp}(t\ t_g g) = \mathrm{lpp}(t\ t_h h) = T$ and $\mathrm{lpp}(\mathbf{u}) \succeq \mathrm{lpp}(t\ t_g\mathbf{v}) \succeq \mathrm{lpp}(t\ t_h\mathbf{w})$ such that we have $\mathrm{lpp}(t(t_g g - ct_h h)) \prec T$. By the hypothesis of the lemma, the S-polynomial $t_g(g^{[\mathbf{v}]}) - ct_h(h^{[\mathbf{w}]}) = (t_g g - ct_h h)^{[t_g\mathbf{v} - ct_h\mathbf{w}]}$ has a standard representation w.r.t. G, that is, there exist $g_i^{[\mathbf{v}_i]} \in G$, such that $t_g g - ct_h h = \sum q_i g_i$, where $\mathrm{lpp}(t_g g - ct_h h) \succeq \mathrm{lpp}(q_i g_i)$ and $\mathrm{lpp}(\mathbf{u}) \succeq \mathrm{lpp}(t\ q_i\mathbf{v}_i)$. Substituting these standard representations back to the original expression of f in (1), we get a new representation for f. Let $T^{(1)}$ be the maximal leading power product of the polynomials appearing in the right side of the new representation. Then we have $T \succ T^{(1)}$. Repeat the above process until $T^{(s)}$ is the same as $\mathrm{lpp}(f)$ for some s after finite steps. Finally, we always get a standard representation for $f^{[\mathbf{u}]}$. □

Lemma 5.2. *Let G be a finite subset of I and $\{f_1^{[\mathbf{e}_1]}, \cdots, f_m^{[\mathbf{e}_m]}\} \subset G$. Then G is a labeled Gröbner basis for I, if for any critical pair $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ of G, the S-polynomial of $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ always has a standard representation w.r.t. G.*

Proof. Using Lemma 5.1, for any $f^{[\mathbf{u}]} \in I$, $f^{[\mathbf{u}]}$ has a standard representation w.r.t. G. By the basic property of standard representations, G is a labeled Gröbner basis for I. □

Before giving a full proof of Theorem 3.4, we introduce the following definitions.

Suppose $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ and $(t_{\bar{f}}, \bar{f}^{[\bar{\mathbf{u}}]}, t_{\bar{g}}, \bar{g}^{[\bar{\mathbf{v}}]})$ are two critical pairs, we say $(t_{\bar{f}}, \bar{f}^{[\bar{\mathbf{u}}]}, t_{\bar{g}}, \bar{g}^{[\bar{\mathbf{v}}]})$ is **smaller** than $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ if one of the following conditions holds:

(a). $\mathrm{lpp}(t_{\bar{f}}\bar{\mathbf{u}}) \prec \mathrm{lpp}(t_f\mathbf{u})$.
(b). $\mathrm{lpp}(t_{\bar{f}}\bar{\mathbf{u}}) = \mathrm{lpp}(t_f\mathbf{u})$ and $\bar{f}^{[\bar{\mathbf{u}}]} < f^{[\mathbf{u}]}$.
(c). $\mathrm{lpp}(t_{\bar{f}}\bar{\mathbf{u}}) = \mathrm{lpp}(t_f\mathbf{u})$, $\bar{f}^{[\bar{\mathbf{u}}]} = f^{[\mathbf{u}]}$ and $\mathrm{lpp}(t_{\bar{g}}\bar{\mathbf{v}}) \prec \mathrm{lpp}(t_g\mathbf{v})$.
(d). $\mathrm{lpp}(t_{\bar{f}}\bar{\mathbf{u}}) = \mathrm{lpp}(t_f\mathbf{u})$, $\bar{f}^{[\bar{\mathbf{u}}]} = f^{[\mathbf{u}]}$, $\mathrm{lpp}(t_{\bar{g}}\bar{\mathbf{v}}) = \mathrm{lpp}(t_g\mathbf{v})$ and $\bar{g}^{[\bar{\mathbf{v}}]} < g^{[\mathbf{v}]}$.

Let D be a set of critical pairs. A critical pair in D is said to be **minimal** if there is no critical pair in D smaller than this critical pair. Remark that the order "smaller" defined on the critical pairs is *a partial order*, i.e. some critical pairs may not be comparable. Thus, the minimal critical pair in D may not be unique, but we can always find one if D is finite.

Now, we give the proof of Theorem 3.4.

Proof of Theorem 3.4. Let G_{end} denote the set returned by the algorithm AGC. According to the hypotheses, G_{end} is finite, and we also have $\{f_1^{[\mathbf{e}_1]}, \cdots, f_m^{[\mathbf{e}_m]}\} \subset G_{end}$ by the algorithm AGC. To show G_{end} is a labeled Gröbner basis for I, we will take the following strategy.

Step 1: Let *Todo* be the set of *all* the critical pairs of G_{end}, and *Done* be an empty set.

Step 2: Select a minimal critical pair $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}] = (t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ in *Todo*.

Step 3: For such $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$, we will prove the following two facts.

(F1). The S-polynomial of $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ has a standard representation w.r.t. G_{end}.
(F2). If $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is *super regular* or *regular*, then $t_f(f^{[\mathbf{u}]})$ is gen-rewritable by G_{end}.

Step 4: Move $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ from $Todo$ to $Done$, i.e. $Todo \longleftarrow Todo \backslash \{[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]\}$ and $Done \longleftarrow Done \cup \{[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]\}$.

We can repeat **Step 2, 3, 4** until $Todo$ is empty. Please note that for every critical pair in $Done$, it always has property (F1); particularly, if this critical pair is super regular or regular, then it has properties (F1) and (F2). When $Todo$ is empty, all the critical pairs of G_{end} will lie in $Done$, and hence, all the corresponding S-polynomials have standard representations w.r.t. G_{end}. Then G_{end} is a labeled Gröbner basis by Lemma 5.2.

Step 1, 2, 4 are trivial, so we next focus on showing the facts in **Step 3**.

Take a minimal critical pair $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}] = (t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ in $Todo$. And this critical pair must appear in the algorithm AGC. Suppose such pair is selected from the set $CPairs$ in some loop of the algorithm AGC and G_k denotes the corresponding set G at the beginning of that loop. For such $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$, it must be in one of the following cases:

C1: $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ is *non-regular*.
C2: $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ is *super regular*.
C3: $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ is *regular* and is *not* gen-rewritable by G_k.
C4: $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ is *regular* and $t_f(f^{[\mathbf{u}]})$ is gen-rewritable by G_k.
C5: $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ is *regular* and $t_g(g^{[\mathbf{v}]})$ is gen-rewritable by G_k.

Thus, to show the facts in **Step 3**, we have two things to do: First, show (F1) holds in case **C1**; Second, show both (F1) and (F2) hold in cases **C2, C3, C4** and **C5**.

We make the following claims under the condition that $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}] = (t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is minimal in $Todo$. The proofs of these claims will be presented after the current proof.

Claim 1: For any $\bar{f}^{[\bar{\mathbf{u}}]} \in I$, if $\bar{f}^{[\bar{\mathbf{u}}]}$'s signature $\prec t_f(f^{[\mathbf{u}]})$'s signature, i.e. $\mathrm{lpp}(\bar{\mathbf{u}}) \prec \mathrm{lpp}(t_f\mathbf{u})$, then $\bar{f}^{[\bar{\mathbf{u}}]}$ has a standard representation w.r.t. G_{end}.

Claim 2: If $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ is super regular or regular and $t_f(f^{[\mathbf{u}]})$ is gen-rewritable by G_{end}, then the S-polynomial of $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ has a standard representation w.r.t. G_{end}.

Claim 3: If $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ is regular and $t_g(g^{[\mathbf{v}]})$ is gen-rewritable by G_{end}, then $t_f(f^{[\mathbf{u}]})$ is also gen-rewritable by G_{end}.

Note that **Claim 2** plays an important role in the whole proof. Since **Claim 2** shows that (F2) implies (F1) in the cases **C2, C3, C4** and **C5**, it suffices to show $t_f(f^{[\mathbf{u}]})$ is gen-rewritable by G_{end} in these cases.

Next, we proceed with each case respectively.

C1: $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ is *non-regular*. Consider the S-polynomial $t_f(f^{[\mathbf{u}]}) - ct_g(g^{[\mathbf{v}]}) = (t_f f - ct_g g)^{[t_f\mathbf{u} - ct_g\mathbf{v}]}$ where $c = \mathrm{lc}(f)/\mathrm{lc}(g)$. Note that $\mathrm{lpp}(t_f\mathbf{u} - ct_g\mathbf{v}) \prec \mathrm{lpp}(t_f\mathbf{u})$ by the definition of non-regular, so **Claim 1** shows $(t_f f - ct_g g)^{[t_f\mathbf{u} - ct_g\mathbf{v}]}$ has a standard representation w.r.t. G_{end}, which proves (F1).

C2: $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ is *super regular*, i.e. $\mathrm{lpp}(t_f\mathbf{u} - ct_g\mathbf{v}) = \mathrm{lpp}(t_f\mathbf{u}) = \mathrm{lpp}(t_g\mathbf{v})$ where $c = \mathrm{lc}(f)/\mathrm{lc}(g)$. Let $\bar{c} := \mathrm{lc}(\mathbf{u})/\mathrm{lc}(\mathbf{v})$. Note that $\bar{c} \neq c$, since $\mathrm{lpp}(t_f\mathbf{u} - ct_g\mathbf{v}) = \mathrm{lpp}(t_f\mathbf{u})$. Then we have $\mathrm{lpp}(t_f f - \bar{c}t_g g) = \mathrm{lpp}(t_f f)$ and $\mathrm{lpp}(t_f\mathbf{u} - \bar{c}t_g\mathbf{v}) \prec \mathrm{lpp}(t_f\mathbf{u})$. So **Claim 1** shows $t_f(f^{[\mathbf{u}]}) - \bar{c}t_g(g^{[\mathbf{v}]}) = (t_f f - \bar{c}t_g g)^{[t_f\mathbf{u} - \bar{c}t_g\mathbf{v}]}$ has a standard representation w.r.t. G_{end}, and hence, there exists $h^{[\mathbf{w}]} \in G_{end}$ such that $\mathrm{lpp}(h)$ divides $\mathrm{lpp}(t_f f - \bar{c}t_g g) = \mathrm{lpp}(t_f f)$ and $\mathrm{lpp}(t_f\mathbf{u}) \succ \mathrm{lpp}(t_f\mathbf{u} - \bar{c}t_g\mathbf{v}) \succeq \mathrm{lpp}(t_h\mathbf{w})$ where $t_h = \mathrm{lpp}(t_f f)/\mathrm{lpp}(h)$. Next, consider

the critical pair $[f^{[\mathbf{u}]}, h^{[\mathbf{w}]}]$. Since $\mathrm{lpp}(t_f f) = \mathrm{lpp}(t_h h)$, the critical pair $[f^{[\mathbf{u}]}, h^{[\mathbf{w}]}]$ has two possible forms.

Form 1: $[f^{[\mathbf{u}]}, h^{[\mathbf{w}]}] = (t_f, f^{[\mathbf{u}]}, t_h, h^{[\mathbf{w}]})$. Since $\mathrm{lpp}(t_f\mathbf{u}) = \mathrm{lpp}(t_g\mathbf{v}) \succ \mathrm{lpp}(t_h\mathbf{w})$, the critical pair $[f^{[\mathbf{u}]}, h^{[\mathbf{w}]}]$ is regular and is smaller than $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ in fashion (c), which means $[f^{[\mathbf{u}]}, h^{[\mathbf{w}]}]$ lies in *Done* and $t_f(f^{[\mathbf{u}]})$ is gen-rewritable by G_{end}.

Form 2: $[f^{[\mathbf{u}]}, h^{[\mathbf{w}]}] = (\bar{t}_f, f^{[\mathbf{u}]}, \bar{t}_h, h^{[\mathbf{w}]})$ where $\bar{t}_f$ divides t_f and $\bar{t}_f \neq t_f$. Since $\mathrm{lpp}(t_f\mathbf{u}) \succ \mathrm{lpp}(t_h\mathbf{w})$, the critical pair $(\bar{t}_f, f^{[\mathbf{u}]}, \bar{t}_h, h^{[\mathbf{w}]})$ is also regular and is smaller than $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ in fashion (a), which means $(\bar{t}_f, f^{[\mathbf{u}]}, \bar{t}_h, h^{[\mathbf{w}]})$ lies in *Done* and $\bar{t}_f(f^{[\mathbf{u}]})$ is gen-rewritable by G_{end}. Then $t_f(f^{[\mathbf{u}]})$ is also gen-rewritable by G_{end}, since $\bar{t}_f$ divides t_f.

C3: $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ is *regular* and *not* gen-rewritable by G_k. According to the algorithm AGC, the S-polynomial $t_f(f^{[\mathbf{u}]}) - ct_g(g^{[\mathbf{v}]})$ is reduced to $h^{[\mathbf{w}]}$ by G_k where $c = \mathrm{lc}(f)/\mathrm{lc}(g)$, and $h^{[\mathbf{w}]}$ will be added to the set G_k at the end of this loop. Note that $G_k \subset G_{end}$ and $h^{[\mathbf{w}]} \in G_{end}$. Since "$<$" is an admissible partial order, we have $h^{[\mathbf{w}]} < f^{[\mathbf{u}]}$ by definition. Combined with the fact $\mathrm{lpp}(\mathbf{w}) = \mathrm{lpp}(t_f\mathbf{u})$, so $t_f(f^{[\mathbf{u}]})$ is gen-rewritable by $h^{[\mathbf{w}]} \in G_{end}$.

C4: $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ is *regular* and $t_f(f^{[\mathbf{u}]})$ is gen-rewritable by G_k. Then $t_f(f^{[\mathbf{u}]})$ is also gen-rewritable by G_{end}, since $G_k \subset G_{end}$.

C5: $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ is *regular* and $t_g(g^{[\mathbf{v}]})$ is gen-rewritable by G_k. $t_g(g^{[\mathbf{v}]})$ is also gen-rewritable by G_{end}, since $G_k \subset G_{end}$. Then **Claim 3** shows $t_f(f^{[\mathbf{u}]})$ is gen-rewritable by G_{end} as well.

Theorem 3.4 is proved. □

We give the proofs for the three claims below.

Proof of **Claim 1**. According to the hypothesis, we have $\bar{f}^{[\bar{\mathbf{u}}]} \in I$ and $\mathrm{lpp}(\bar{\mathbf{u}}) \prec \mathrm{lpp}(t_f\mathbf{u})$. So for any critical pair $(t_{f'}, f'^{[\mathbf{u}']}, t_{g'}, g'^{[\mathbf{v}']})$ of G_{end} with $\mathrm{lpp}(\bar{\mathbf{u}}) \succeq \mathrm{lpp}(t_{f'}\mathbf{u}')$, the critical pair $(t_{f'}, f'^{[\mathbf{u}']}, t_{g'}, g'^{[\mathbf{v}']})$ is smaller than $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ in fashion (a) and hence lies in *Done*, which means the S-polynomial of $(t_{f'}, f'^{[\mathbf{u}']}, t_{g'}, g'^{[\mathbf{v}']})$ has a standard representation w.r.t. G_{end}. So Lemma 5.1 shows that $\bar{f}^{[\bar{\mathbf{u}}]}$ has a standard representation w.r.t. G_{end}. □

Proof of **Claim 2**. We have that $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}] = (t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is minimal in *Todo* and $t_f(f^{[\mathbf{u}]})$ is gen-rewritable by G_{end}. Let $c := \mathrm{lc}(f)/\mathrm{lc}(g)$. Then $\bar{f}^{[\bar{\mathbf{u}}]} = t_f(f^{[\mathbf{u}]}) - ct_g(g^{[\mathbf{v}]}) = (t_f f - ct_g g)^{[t_f\mathbf{u} - ct_g\mathbf{v}]}$ is the S-polynomial of $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$. Since $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ is super regular or regular, we have $\mathrm{lpp}(\bar{\mathbf{u}}) = \mathrm{lpp}(t_f\mathbf{u})$. Next we will show that $\bar{f}^{[\bar{\mathbf{u}}]}$ has a standard representation w.r.t. G_{end}. The proof is organized as follows.

First: We show that there exists $f_0^{[\mathbf{u}_0]} \in G_{end}$ such that $f_0^{[\mathbf{u}_0]} < f^{[\mathbf{u}]}$, $t_f(f^{[\mathbf{u}]})$ is gen-rewritable by $f_0^{[\mathbf{u}_0]}$ and $t_0(f_0^{[\mathbf{u}_0]})$ is *not* gen-rewritable by G_{end} where $t_0 = \mathrm{lpp}(t_f\mathbf{u})/\mathrm{lpp}(\mathbf{u}_0)$.

Second: For such $f_0^{[\mathbf{u}_0]}$, we show that $\mathrm{lpp}(\bar{f}) \succeq \mathrm{lpp}(t_0 f_0)$ where $t_0 = \mathrm{lpp}(t_f\mathbf{u})/\mathrm{lpp}(\mathbf{u}_0)$.

Third: We prove that $\bar{f}^{[\bar{\mathbf{u}}]}$ has a standard representation w.r.t. G_{end}.

Proof of the **First** fact. By hypothesis, suppose $t_f(f^{[\mathbf{u}]})$ is gen-rewritable by some $f_1^{[\mathbf{u}_1]} \in G_{end}$, i.e. $\mathrm{lpp}(\mathbf{u}_1)$ divides $\mathrm{lpp}(t_f\mathbf{u})$ and $f_1^{[\mathbf{u}_1]} < f^{[\mathbf{u}]}$. Let $t_1 := \mathrm{lpp}(t_f\mathbf{u})/\mathrm{lpp}(\mathbf{u}_1)$. If $t_1(f_1^{[\mathbf{u}_1]})$ is not gen-rewritable by G_{end}, then $f_1^{[\mathbf{u}_1]}$ is the polynomial we are looking for. Otherwise,

there exists $f_2^{[\mathbf{u}_2]} \in G_{end}$ such that $t_1(f_1^{[\mathbf{u}_1]})$ is gen-rewritable by $f_2^{[\mathbf{u}_2]}$. Note that $t_f(f^{[\mathbf{u}]})$ is also gen-rewritable by $f_2^{[\mathbf{u}_2]}$ and we have $f^{[\mathbf{u}]} > f_1^{[\mathbf{u}_1]} > f_2^{[\mathbf{u}_2]}$. Let $t_2 := \mathrm{lpp}(t_f\mathbf{u})/\mathrm{lpp}(\mathbf{u}_2)$. We next discuss whether $t_2(f_2^{[\mathbf{u}_2]})$ is gen-rewritable by G_{end}. In the better case, $f_2^{[\mathbf{u}_2]}$ is the desired polynomial if $t_2(f_2^{[\mathbf{u}_2]})$ is not gen-rewritable by G_{end}; while in the worse case, $t_2(f_2^{[\mathbf{u}_2]})$ is gen-rewritable by some $f_3^{[\mathbf{u}_3]} \in G_{end}$. We can repeat the above discussions for the worse case. Finally, we will get a chain $f^{[\mathbf{u}]} > f_1^{[\mathbf{u}_1]} > f_2^{[\mathbf{u}_2]} > \cdots$. This chain must terminate, since G_{end} is finite and ">" is a partial order defined on G_{end}. Suppose $f_s^{[\mathbf{u}_s]}$ is the last one in the above chain. Then $t_f(f^{[\mathbf{u}]})$ is gen-rewritable by $f_s^{[\mathbf{u}_s]}$ and $t_s(f_s^{[\mathbf{u}_s]})$ is not gen-rewritable by G_{end} where $t_s = \mathrm{lpp}(t_f\mathbf{u})/\mathrm{lpp}(\mathbf{u}_s)$.

Proof of the **Second** fact. From the **First** fact, we have that $t_0(f_0^{[\mathbf{u}_0]})$ is *not* gen-rewritable by G_{end} where $t_0 = \mathrm{lpp}(t_f\mathbf{u})/\mathrm{lpp}(\mathbf{u}_0)$. Next, we prove the **Second** fact by contradiction. Assume $\mathrm{lpp}(\bar{f}) \prec \mathrm{lpp}(t_0f_0)$. Let $c_0 := \mathrm{lc}(\bar{\mathbf{u}})/\mathrm{lc}(\mathbf{u}_0)$. Then for the polynomial $\bar{f}^{[\bar{\mathbf{u}}]} - c_0t_0(f_0^{[\mathbf{u}_0]}) = (\bar{f} - c_0t_0f_0)^{[\bar{\mathbf{u}}-c_0t_0\mathbf{u}_0]}$, we have $\mathrm{lpp}(\bar{f} - c_0t_0f_0) = \mathrm{lpp}(t_0f_0)$ and $\mathrm{lpp}(\bar{\mathbf{u}} - c_0t_0\mathbf{u}_0) \prec \mathrm{lpp}(\bar{\mathbf{u}}) = \mathrm{lpp}(t_0\mathbf{u}_0) = \mathrm{lpp}(t_f\mathbf{u})$. So $(\bar{f} - c_0t_0f_0)^{[\bar{\mathbf{u}}-c_0t_0\mathbf{u}_0]}$ has a standard representation w.r.t. G_{end} by **Claim 1**, and hence, there exists $h^{[\mathbf{w}]} \in G_{end}$ such that $\mathrm{lpp}(h)$ divides $\mathrm{lpp}(\bar{f} - c_0t_0f_0) = \mathrm{lpp}(t_0f_0)$ and $\mathrm{lpp}(t_0\mathbf{u}_0) \succ \mathrm{lpp}(\bar{\mathbf{u}} - c_0t_0\mathbf{u}_0) \succeq \mathrm{lpp}(t_h\mathbf{w})$ where $t_h = \mathrm{lpp}(t_0f_0)/\mathrm{lpp}(h)$. Next consider the critical pair $[f_0^{[\mathbf{u}_0]}, h^{[\mathbf{w}]}]$. Similarly, since $\mathrm{lpp}(t_0f_0) = \mathrm{lpp}(t_hh)$, the critical pair $[f_0^{[\mathbf{u}_0]}, h^{[\mathbf{w}]}]$ has two possible forms.

Form 1: $[f_0^{[\mathbf{u}_0]}, h^{[\mathbf{w}]}] = (t_0, f_0^{[\mathbf{u}_0]}, t_h, h^{[\mathbf{w}]})$. Since $\mathrm{lpp}(t_0\mathbf{u}_0) \succ \mathrm{lpp}(t_h\mathbf{w})$, the critical pair $[f_0^{[\mathbf{u}_0]}, h^{[\mathbf{w}]}]$ is regular and is smaller than $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ in fashion (b), which means $[f_0^{[\mathbf{u}_0]}, h^{[\mathbf{w}]}]$ lies in *Done* and $t_0(f_0^{[\mathbf{u}_0]})$ is gen-rewritable by G_{end}, which contradicts with the property that $t_0(f_0^{[\mathbf{u}_0]})$ is *not* gen-rewritable by G_{end}.

Form 2: $[f_0^{[\mathbf{u}_0]}, h^{[\mathbf{w}]}] = (\bar{t}_0, f_0^{[\mathbf{u}_0]}, \bar{t}_h, h^{[\mathbf{w}]})$ where $\bar{t}_0$ divides t_0 and $\bar{t}_0 \neq t_0$. Since $\mathrm{lpp}(t_0\mathbf{u}_0) \succ \mathrm{lpp}(t_h\mathbf{w})$, the critical pair $(\bar{t}_0, f_0^{[\mathbf{u}_0]}, \bar{t}_h, h^{[\mathbf{w}]})$ is also regular and is smaller than $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ in fashion (a), which means $(\bar{t}_0, f_0^{[\mathbf{u}_0]}, \bar{t}_h, h^{[\mathbf{w}]})$ lies in *Done* and $\bar{t}_0(f_0^{[\mathbf{u}_0]})$ is gen-rewritable by G_{end}. Then $t_0(f_0^{[\mathbf{u}_0]})$ is also gen-rewritable by G_{end}, since $\bar{t}_0$ divides t_0. This is also contradicts with the property that $t_0(f_0^{[\mathbf{u}_0]})$ is *not* gen-rewritable by G_{end}.

In either case, the **Second** fact is proved.

Proof of the **Third** fact. According to the second fact, we have $\mathrm{lpp}(\bar{f}) \succeq \mathrm{lpp}(t_0f_0)$ where $t_0 = \mathrm{lpp}(t_f\mathbf{u})/\mathrm{lpp}(\mathbf{u}_0)$. Let $c_0 := \mathrm{lc}(\bar{\mathbf{u}})/\mathrm{lc}(\mathbf{u}_0)$. For the polynomial $\bar{f}^{[\bar{\mathbf{u}}]} - c_0t_0(f_0^{[\mathbf{u}_0]}) = (\bar{f} - c_0t_0f_0)^{[\bar{\mathbf{u}}-c_0t_0\mathbf{u}_0]}$, we have $\mathrm{lpp}(\bar{f} - c_0t_0f_0) \preceq \mathrm{lpp}(\bar{f})$ and $\mathrm{lpp}(\bar{\mathbf{u}} - c_0t_0\mathbf{u}_0) \prec \mathrm{lpp}(\bar{\mathbf{u}})$. So $(\bar{f} - c_0t_0f_0)^{[\bar{\mathbf{u}}-c_0t_0\mathbf{u}_0]}$ has a standard representation w.r.t. G_{end} by **Claim 1**. Note that $\mathrm{lpp}(\bar{f}) \succeq \mathrm{lpp}(t_0f_0)$ and $\mathrm{lpp}(\bar{\mathbf{u}}) = \mathrm{lpp}(t_0\mathbf{u}_0)$. So after adding $c_0t_0f_0$ to both sides of the standard representation of $\bar{f}^{[\bar{\mathbf{u}}]} - c_0t_0(f_0^{[\mathbf{u}_0]})$, then we will get a standard representation of $\bar{f}^{[\bar{\mathbf{u}}]}$ w.r.t. G_{end}. □

Proof of **Claim 3**. Since $t_g(g^{[\mathbf{v}]})$ is gen-rewritable by G_{end} and $\mathrm{lpp}(t_g\mathbf{v}) \prec \mathrm{lpp}(t_f\mathbf{u})$, by using a similar method in the proof of the First and Second facts in **Claim 2**, we have that there exists $g_0^{[\mathbf{v}_0]} \in G_{end}$ such that $t_g(g^{[\mathbf{v}]})$ is gen-rewritable by $g_0^{[\mathbf{v}_0]}$, $t_0(g_0^{[\mathbf{v}_0]})$ is not gen-rewritable by G_{end} and $\mathrm{lpp}(t_gg) \succeq \mathrm{lpp}(t_0g_0)$ where $t_0 = \mathrm{lpp}(t_g\mathbf{v})/\mathrm{lpp}(\mathbf{v}_0)$.

If $\mathrm{lpp}(t_0g_0) = \mathrm{lpp}(t_gg) = \mathrm{lpp}(t_ff)$, then the critical pair $[f^{[\mathbf{u}]}, g_0^{[\mathbf{v}_0]}]$ has two possible forms.

Form 1: $[f^{[\mathbf{u}]}, g_0^{[\mathbf{v}_0]}] = (t_f, f^{[\mathbf{u}]}, t_0, g_0^{[\mathbf{v}_0]})$. Since $\mathrm{lpp}(t_f\mathbf{u}) \succ \mathrm{lpp}(t_g\mathbf{v}) = \mathrm{lpp}(t_0\mathbf{v}_0)$, the critical pair $[f^{[\mathbf{u}]}, g_0^{[\mathbf{v}_0]}]$ is regular and is smaller than $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ in fashion (d), which means $[f^{[\mathbf{u}]}, g_0^{[\mathbf{v}_0]}]$ lies in *Done* and $t_f(f^{[\mathbf{u}]})$ is gen-rewritable by G_{end}.

Form 2: $[f^{[\mathbf{u}]}, g_0^{[\mathbf{v}_0]}] = (\bar{t}_f, f^{[\mathbf{u}]}, \bar{t}_0, g_0^{[\mathbf{v}_0]})$ where $\bar{t}_f$ divides t_f and $\bar{t}_f \neq t_f$. Since $\mathrm{lpp}(t_f\mathbf{u}) \succ \mathrm{lpp}(t_g\mathbf{v}) = \mathrm{lpp}(t_0\mathbf{v}_0)$, the critical pair $(\bar{t}_f, f^{[\mathbf{u}]}, \bar{t}_0, g_0^{[\mathbf{v}_0]})$ is also regular and is smaller than $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ in fashion (a), which means $(\bar{t}_f, f^{[\mathbf{u}]}, \bar{t}_0, g_0^{[\mathbf{v}_0]})$ lies in *Done* and $\bar{t}_f(f^{[\mathbf{u}]})$ is gen-rewritable by G_{end}. Then $t_f(f^{[\mathbf{u}]})$ is also gen-rewritable by G_{end}, since $\bar{t}_f$ divides t_f.

Otherwise, $\mathrm{lpp}(t_gg) \succ \mathrm{lpp}(t_0g_0)$ holds. Let $c := \mathrm{lc}(\mathbf{v})/\mathrm{lc}(\mathbf{v}_0)$. For the polynomial $t_gg^{[\mathbf{v}]} - ct_0(g_0^{[\mathbf{v}_0]}) = (t_gg - ct_0g_0)^{[t_g\mathbf{v}-ct_0\mathbf{v}_0]}$, we have $\mathrm{lpp}(t_gg - ct_0g_0) = \mathrm{lpp}(t_gg)$ and $\mathrm{lpp}(t_g\mathbf{v} - ct_0\mathbf{v}_0) \prec \mathrm{lpp}(t_g\mathbf{v})$. Then $(t_gg - ct_0g_0)^{[t_g\mathbf{v}-ct_0\mathbf{v}_0]}$ has a standard representation w.r.t. G_{end} by **Claim 1**, and hence, there exists $h^{[\mathbf{w}]} \in G_{end}$ such that $\mathrm{lpp}(h)$ divides $\mathrm{lpp}(t_gg - ct_0g_0) = \mathrm{lpp}(t_gg)$ and $\mathrm{lpp}(t_h\mathbf{w}) \preceq \mathrm{lpp}(t_g\mathbf{v} - ct_0\mathbf{v}_0) \prec \mathrm{lpp}(t_g\mathbf{v})$ where $t_h = \mathrm{lpp}(t_gg)/\mathrm{lpp}(h)$. Note that $\mathrm{lpp}(t_hh) = \mathrm{lpp}(t_gg) = \mathrm{lpp}(t_ff)$. The critical pair of $[f^{[\mathbf{u}]}, h^{[\mathbf{w}]}]$ also has two possible forms.

Form 1: $[f^{[\mathbf{u}]}, h^{[\mathbf{w}]}] = (t_f, f^{[\mathbf{u}]}, t_h, h^{[\mathbf{w}]})$. Since $\mathrm{lpp}(t_f\mathbf{u}) \succ \mathrm{lpp}(t_g\mathbf{v}) \succ \mathrm{lpp}(t_h\mathbf{w})$, the critical pair $[f^{[\mathbf{u}]}, h^{[\mathbf{w}]}]$ is regular and is smaller than $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ in fashion (c), which means $[f^{[\mathbf{u}]}, h^{[\mathbf{w}]}]$ lies in *Done* and $t_f(f^{[\mathbf{u}]})$ is gen-rewritable by G_{end}.

Form 2: $[f^{[\mathbf{u}]}, h^{[\mathbf{w}]}] = (\bar{t}_f, f^{[\mathbf{u}]}, \bar{t}_h, h^{[\mathbf{w}]})$ where $\bar{t}_f$ divides t_f and $\bar{t}_f \neq t_f$. Since $\mathrm{lpp}(t_f\mathbf{u}) \succ \mathrm{lpp}(t_g\mathbf{v}) \succ \mathrm{lpp}(t_h\mathbf{w})$, the critical pair $(\bar{t}_f, f^{[\mathbf{u}]}, \bar{t}_h, h^{[\mathbf{w}]})$ is also regular and is smaller than $[f^{[\mathbf{u}]}, g^{[\mathbf{v}]}]$ in fashion (a), which means $(\bar{t}_f, f^{[\mathbf{u}]}, \bar{t}_h, h^{[\mathbf{w}]})$ lies in *Done* and $\bar{t}_f(f^{[\mathbf{u}]})$ is gen-rewritable by G_{end}. Then $t_f(f^{[\mathbf{u}]})$ is also gen-rewritable by G_{end}, since $\bar{t}_f$ divides t_f.

Claim 3 is proved. □

Remark 5.3. *The proof of Theorem 3.4 also indicates that, all regular or super regular critical pairs of G_{end} are gen-rewritable by G_{end}.*

6. Developing New Criteria

Based on the generalized criterion, to develop new criteria for signature-based algorithms, it suffices to choose appropriate admissible partial orders for the generalized criterion.

For example, we can develop a new criterion by using the following admissible partial order implied by GVW's criteria: for any $f^{[\mathbf{u}]}, g^{[\mathbf{v}]} \in G$, we say $g^{[\mathbf{v}]} < f^{[\mathbf{u}]}$ if one of the following two conditions holds:

1. $\mathrm{lpp}(t'g) < \mathrm{lpp}(tf)$, where $t' = \frac{\mathrm{lcm}(\mathrm{lpp}(\mathbf{u}),\mathrm{lpp}(\mathbf{v}))}{\mathrm{lpp}(\mathbf{v})}$ and $t = \frac{\mathrm{lcm}(\mathrm{lpp}(\mathbf{u}),\mathrm{lpp}(\mathbf{v}))}{\mathrm{lpp}(\mathbf{u})}$ such that $t(f^{[\mathbf{u}]})$ and $t'(g^{[\mathbf{v}]})$ have the same signature, i.e. $\mathrm{lpp}(t\mathbf{u}) = \mathrm{lpp}(t'\mathbf{v})$.
2. $\mathrm{lpp}(t'g) = \mathrm{lpp}(tf)$ and $g^{[\mathbf{v}]}$ is added to G later than $f^{[\mathbf{u}]}$.

Recently, we notice Huang also considers a similar order in (Huang, 2010). Applying this admissible partial order in the generalized criterion of algorithm AGC, we get a new algorithm (named by NEW). This algorithm can be regarded as an improved version of GVW.

To test the efficacy of the new criterion, we implemented the algorithm NEW on Singular (version 3-1-2), and use two strategies for selecting critical pairs.

Minimal **S**ignature Strategy: $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is selected from *CPairs* only if there does *not* exist another critical pair $(t_{\bar{f}}, \bar{f}^{[\bar{\mathbf{u}}]}, t_{\bar{g}}, \bar{g}^{[\bar{\mathbf{v}}]}) \in$ *CPairs* such that $\mathrm{lpp}(t_{\bar{f}}\bar{\mathbf{u}}) \prec \mathrm{lpp}(t_f\mathbf{u})$;

Minimal **D**egree Strategy: $(t_f, f^{[\mathbf{u}]}, t_g, g^{[\mathbf{v}]})$ is selected from *CPairs* if there does *not* exist another critical pair $(t_{\bar{f}}, \bar{f}^{[\bar{\mathbf{u}}]}, t_{\bar{g}}, \bar{g}^{[\bar{\mathbf{v}}]}) \in$ *CPairs* such that $\deg(\mathrm{lpp}(t_{\bar{f}}\bar{f})) \prec \deg(\mathrm{lpp}(t_f f))$. The proofs in Section 5 ensure the algorithm NEW is correct for both strategies.

In the following table, we use (s) and (d) to refer the two strategies respectively. The order $\prec_1$ is the Graded Reverse Lex order and $\prec_2$ is extended from $\prec_1$ in the following way: $x^\alpha \mathbf{e}_i \prec_2 x^\beta \mathbf{e}_j$, if either $\mathrm{lpp}(x^\alpha f_i) \prec_1 \mathrm{lpp}(x^\beta f_j)$, or $\mathrm{lpp}(x^\alpha f_i) = \mathrm{lpp}(x^\beta f_j)$ and $i > j$. This order $\prec_2$ has also been used in (Gao et al., 2010b; Sun and Wang, 2010b). The examples are selected from (Gao et al., 2010b) and the timings are obtained on Core i5 4×2.8 GHz with 4GB memory running Windows 7.

Table 1: *#all.*: number of all critical pairs generated in the computation; *#red.*: number of critical pairs that are really reduced in the computation; *#gen.*: number of non-zero generators in the Gröbner basis in the last iteration but before computing a reduced Gröbner basis. "Katsura5 (22)" means there are 22 non-zero generators in the reduced Gröbner basis of Katsura5.

	NEW(s)	NEW(d)	NEW(s)	NEW(d)	NEW(s)	NEW(d)
	Katsura5 (22)		Katsura6 (41)		Katsura7 (74)	
#all.	351	378	1035	1275	3160	3160
#red.	39	40	73	78	121	121
#gen.	27	28	46	51	80	80
time(sec.)	1.400	1.195	7.865	5.650	38.750	29.950
	Katsura8 (143)		Cyclic5 (20)		Cyclic6 (45)	
#all.	11325	11325	1128	2080	18528	299925
#red.	244	244	56	78	231	834
#gen.	151	151	48	65	193	775
time(sec.)	395.844	310.908	2.708	2.630	106.736	787.288

From the above table, we can see that the new criterion can reject redundant critical pairs effectively. We also notice that the timings are influenced by the strategies of selecting critical pairs. For some examples, the algorithm with minimal signature strategy has better performance. The possible reason is that less critical pairs are generated by this strategy. For other examples, the algorithm with minimal degree strategy cost less time. The possible reason is that, although the algorithm with the minimal degree strategy usually generates more critical pairs, the critical pairs which are really needed to be reduced usually have lower degrees.

7. Conclusions and Future works

Signature-based algorithms are a popular kind of algorithms for computing Gröbner basis. A generalized criterion for signature-based algorithms is proposed in this paper. Almost all

existing criteria of signature-based algorithms can be specialized by the generalized criterion, and we show in detail how the generalized criterion specializes to F5 and GVW's criteria. We also proved that if the partial order is admissible, the generalized criterion is always correct no matter which computing order of the critical pairs is used. Since the generalized criterion can specialize to F5 and GVW's criteria, the proof in this paper also ensures the correctness of F5 and GVW for any computing order of critical pairs.

The significance of this generalized criterion is to describe which kind of criterion is correct in signature-based algorithms. Moreover, the generalized criterion also provides an effective approach to check and develop new criteria for signature-based algorithms, i.e., if a new criterion can be specialized from the generalized criterion by using an admissible partial order, it must be correct; when developing new criteria, it suffices to choose admissible partial orders in the generalized criterion. We also develop a new effective criterion in this paper. We believe that if the admissible partial order is in fact a total order, then the generalized criterion can reject almost all useless critical pairs. The proof of the claim will be included in future works.

Note that the generalized criterion is just one application of Key Fact in Section 2. We believe more results can be deduced from Key Fact as well. Related works will also be included in our future papers.

However, there are still some open problems.

Problem 1: Is the generalized criterion still correct if the partial order is not admissible? We do know some partial orders lead to wrong criteria. For example, consider the following partial order which is not admissible: for any $f^{[\mathbf{u}]}, g^{[\mathbf{v}]} \in G$, we say $g^{[\mathbf{v}]} < f^{[\mathbf{u}]}$, if $g = 0$ and $f \neq 0$; otherwise, $g^{[\mathbf{v}]}$ is added to G ***earlier*** than $f^{[\mathbf{u}]}$. This partial order leads to a wrong criterion. Because the polynomials $f_1^{[\mathbf{e}_1]}, \cdots, f_m^{[\mathbf{e}_m]}$ are added to G earlier than others, so using this partial order, the generalized criterion will reject almost all critical pairs that are generated later, which definitely leads to a wrong output unless $\{f_1^{[\mathbf{e}_1]}, \cdots, f_m^{[\mathbf{e}_m]}\}$ itself is a labeled Gröbner basis.

Problem 2: Does the labeled Gröbner basis always exist for any ideal? Clearly, if the algorithm AGC terminates, then labeled Gröbner basis always exists. Note that GVW also computes a labeled Gröbner basis, and recently we learn by private communication about that Gao et al. have proved the termination of GVW, so in that sense the existence of labeled Gröbner basis has also been proved.

Problem 3: Does the algorithm AGC always terminate in finite steps? Since GVW has a special demand on the computing order of critical pairs, the proof for the termination of GVW cannot ensure the termination of the algorithm AGC. However, after testing many examples, we have not found a counterexample that AGC does not terminate.

References

M. Albrecht and J. Perry. F4/5. Preprint, arXiv:1006.4933v2 [math.AC], 2010.

A. Arri and J. Perry. The F5 criterion revised. Preprint, arXiv:1012.3664v3 [math.AC], 2010.

B. Buchberger. A criterion for detecting unnecessary reductions in the construction of Gröbner basis. In Proceedings of EUROSAM'79, Lect. Notes in Comp. Sci., Springer, Berlin, vol. 72, 3-21, 1979.

B. Buchberger. Gröbner-bases: an algorithmic method in polynomial ideal theory. Reidel Publishing Company, Dodrecht - Boston - Lancaster, 1985.
N. Courtois, A. Klimov, J. Patarin, and A. Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In Proceedings of EUROCRYPT'00, Lect. Notes in Comp. Sci., Springer, Berlin, vol. 1807, 392-407, 2000.
D. Cox, J. Little, and D. O'Shea. Using algebraic geometry. Springer, New York, second edition, 2005.
J. Ding, J. Buchmann, M.S.E. Mohamed, W.S.A.E. Mohamed, and R.-P. Weinmann. MutantXL. In Proceedings of the 1st international conference on Symbolic Computation and Cryptography (SCC08), Beijing, China, 16-22, 2008.
C. Eder. On the criteria of the F5 algorithm. Preprint, arXiv:0804.2033v4 [math.AC], 2008.
C. Eder and J. Perry. F5C: a variant of Faugère's F5 algorithm with reduced Gröbner bases. J. Symb. Comput., vol. 45(12), 1442-1458, 2010.
C. Eder and J. Perry. Signature-based Algorithms to Compute Gröbner Bases. In Proceedings of ISSAC'11, ACM Press, New York, USA, 99-106, 2011.
J.-C. Faugère. A new effcient algorithm for computing Gröbner bases (F_4). J. Pure Appl. Algebra, vol. 139(1-3), 61-88, 1999.
J.-C. Faugère. A new effcient algorithm for computing Gröbner bases without reduction to zero (F_5). In Proceedings of ISSAC'02, ACM Press, New York, USA, 75-82, 2002. Revised version downloaded from fgbrs.lip6.fr/jcf/Publications/index.html.
S.H. Gao, Y.H. Guan, and F. Volny. A new incremental algorithm for computing Gröbner bases. In Proceedings of ISSAC'10, ACM Press, New York, USA, 13-19, 2010.
S.H. Gao, F. Volny, and M.S. Wang. A new algorithm for computing Gröbner bases. Cryptology ePrint Archive, Report 2010/641, 2010.
R. Gebauer and H.M. Moller. Buchberger's algorithm and staggered linear bases. In Proceedings of SYMSAC'86, ACM press, New York, USA, 218-221, 1986.
A. Giovini, T. Mora, G. Niesi, L. Robbiano and C. Traverso. "One sugar cube, please" or selection strategies in the Buchberger algorithm. In Proceedings of ISSAC'91, ACM Press, New York, USA, 49-54, 1991.
A. Hashemi and G. Ars. Extended F5 criteria. J. Symb. Comput., vol. 45(12), 1330-1340, 2010.
L. Huang. A new conception for computing Gröbner basis and its applications. Preprint, arXiv:1012.5425v2 [cs.SC], 2010.
D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In Proceeding of EUROCAL'83, Lect. Notes in Comp. Sci., Springer, Berlin, vol. 162, 146-156, 1983.
H.M. Möller, T. Mora, and C. Traverso. Gröbner bases computation using syzygies. In Proceedings of ISSAC'92, ACM Press, New York, USA, 320-328, 1992.
T. Stegers. Faugère's F5 algorithm revisited. Cryptology ePrint Archive, Report 2006/404, 2006.
Y. Sun and D.K. Wang. The F5 algorithm in Buchberger's style. To appear in J. Syst. Sci. Complex., arXiv:1006.5299v2 [cs.SC], 2010.
Y. Sun and D.K. Wang. A new proof for the correctness of the F5 algorithm. Preprint, arXiv:1004.0084v4 [cs.SC], 2010.
Y. Sun and D.K. Wang. A Generalized Criterion for Signature Related Gröbner Basis Algorithms. In Proceedings of ISSAC'11, ACM Press, New York, USA, 337-344, 2011.
A. Zobnin. Generalization of the F5 algorithm for calculating Gröbner bases for polynomial ideals. Programming and Computer Software, vol. 36(2), 75-82, 2010.